

# CERTIFIED HEALTHCARE INFORMATION SYSTEMS SECURITY PRACTITIONER

([CLICK HERE TO VIEW THE COURSE LISTING ON NICCS.US-CERT.GOV](#))

**October 15<sup>th</sup> – October 18<sup>th</sup>, 2018**



## COURSE DESCRIPTION

The Mile2 Certified Healthcare Information Systems Security Practitioner vendor-neutral certification course was developed because of growing industry regulations and privacy requirements in the healthcare industry. The CHISSP's have become vital in managing and protecting healthcare data and tasked to protect patient information by implementing, managing, and assessing proper IT controls for patient health information integrity. This certification course covers the skills and knowledge to implement the best IT Healthcare Practices, as well as regulatory compliance and standards in the healthcare industry.



## TRAINING LOCATION

**Center for Applied Cyber Education**  
11935 Abercorn Street, Savannah, GA 31419



**YOUR CYBER SECURITY CAREER BEGINS HERE**

## LEARNING OBJECTIVES

1. Introduction to the Healthcare Industry
2. The Regulatory Environment
3. HIPPA, HITECH and GAPP
4. Privacy and Security in Healthcare
5. Governance and Risk Management
6. Remediation Action Plans
7. Information Risk Assessment
8. Third-Party Risk Management
9. Information Flow Mapping and Scope
10. Asset Protection Controls

## COURSE FEES INCLUDE

**Materials:** **Hard Copy** (Provided at Training Location)

- Course Text / Workbook
- Text: Key Security Concepts & Definitions
- Text: Exam Prep Guide
- Cool SWAG

**Electronic** (Loaded in Student Account)

\* Access to digital content for 1-year

- Course Text / Workbook
- Course Video Series
- CEU Completion Certificate
- Course Prep Guide
- Course Exam Simulator

**Exam Voucher**

- Re-Take Exam Voucher (if needed)



A 15% discount is available for all members of our military affiliated communities. For information on how to receive a discount code, please contact Scott C. Scheidt:

[cyber@georgiasouthern.edu](mailto:cyber@georgiasouthern.edu)

## STUDENT COURSE FEE:

(BEFORE DISCOUNT)

**\$2,500**

## REGISTER NOW FOR YOUR CYBER SECURITY CERTIFICATION

### Electronic Registration & Payment

Link: [https://touchnet.georgiasouthern.edu/C20795\\_ustores/web/classic/product\\_detail.jsp?PRODUCTID=1509](https://touchnet.georgiasouthern.edu/C20795_ustores/web/classic/product_detail.jsp?PRODUCTID=1509)

### Check / Purchase Order (Please contact Scott C. Scheidt via email or phone.)

- PHONE: (912) 344-2750
- EMAIL: [cyber@georgiasouthern.edu](mailto:cyber@georgiasouthern.edu)



## ABOUT THE INSTRUCTOR

Teresa Townsend has an Associates of Technology Degree of Computer Information Systems Networking Specialist. She has worked for over five years at [Coastal Regional Commission](#) as an Administrative/IT Assistant. Prior to that, she worked for 27 years for Health Department Home Care Services in a variety of positions including Computer Network Administrator and Administrative Operations Manager. Teresa was also part of the adjunct faculty at Altamaha Technical College, teaching a number of computer networking classes. To reach Teresa by email, click [HERE](#).

## DETAILED COURSE DESCRIPTION

### Module 1: Healthcare Industry Overview

Introduction	Health Insurance Portability and Accountability Act
The Healthcare Industry	Healthcare Data Management
The Healthcare Environment	Clinical Research
Various Healthcare Sectors	Patient Care and Safety
Information Technology in Healthcare	External Third Parties
Digital Health Records	Vendors
Health Information Exchange	Business Partners
Healthcare Insurance	Data Sharing
Medical Classification	Health Information Management Process
Billing, Payment and Reimbursement	Health Data Characterization
Workflow Management	Legal Medical Records

### Module 2: The Regulatory Environment

Introduction	Copyrights
Identifying Applicable Regulations	Trade Secrets
Security, Privacy and Legal Issues	Treaties
Data Breach Regulations	Mental Health
Personally Identifiable Information (PII)	Substance Abuse
Information Flow Mapping	Pregnancy
Jurisdictional Implications	Human Immunodeficiency Syndrome (HIV)
Data Subjects	HIPPA
Data Owners	HITECH
Data Custodians	Types of Security Policies
Data Controllers	Standards
Data Processors	Baselines
Common Law	Procedures
Criminal Law	Guidelines
Tort Law	Healthcare Documentation
Administrative Law	ISO 27000 Series
Civil Law	National Institute of Standards and Technology (NIST)
Customary Law	Common Criteria
Religious Law	IG Toolkit
Hybrid Law	Generally Accepted Privacy Principles (GAPP)
Laws and Liability	Compensating Controls
Intellectual Property Laws	Control Variance
Patents	Residual Risk Tolerance
Trademarks	Organizational Code of Ethics

### Module 3: Privacy and Security in Healthcare

Introduction	Purpose Specification
Confidentiality	Disclosure Limitation
Integrity	Transfer to Third Parties
Availability	Trans-Border Concerns
Access Control	Access Limitation
Data Encryption	Types of Security
Training and Awareness	Accuracy, Completeness and Quality Management
Logging and Monitoring	Designation of a Privacy Officer
Vulnerability Management	Transparency and Openness

System Recovery  
Segregation of Duties  
Least Privilege  
Business Continuity  
Data Retention and Destruction  
Consent and Choice  
Limited Collection  
Legitimate Purpose

Additional Measures for Breach Notification  
Dependency  
Integration  
Personal/Health Information Protected by Law  
Sensitivity Mitigation  
Mental Health  
Notice and Purpose Specification  
Healthcare Security and Privacy Terminology

#### **Module 4: Information Governance and Risk Management**

Introduction  
Information Governance  
Approach to Governance Structures  
Information Asset Identification  
Asset Valuation  
Vulnerability  
Exposure  
Threats  
Likelihood  
Impact  
Risk  
Controls  
Residual Risk

Risk Acceptance  
NIST  
CMS  
ISO 27000  
Remediation Action Plans  
Risk Mitigation and Remediation  
Risk Transfer  
Risk Acceptance  
Risk Avoidance  
Organizational Communications  
Exception Handling  
Reporting and Metrics

#### **Module 5: Information Risk Assessment**

Introduction  
Risk Assessment  
The Information Lifecycle  
Tools, Resources and Techniques  
Desired Outcomes  
Control Frameworks  
Information Gathering  
Estimated Timelines for Risk Remediation

Gap Analysis  
Corrective Action Plans  
Mitigation Actions  
Types of Controls  
Administrative Controls  
Operational/Physical Controls  
Technical/Logical Controls  
Controls Related to Time

#### **Module 6: Third-Party Risk Management**

Introduction  
Third Parties  
Information: Use, Processing, Storage, Transmission  
Third-Party Roles and Relationships  
Implication of Global Trade Restrictions  
Organizational Requirements  
Triggers Leading to Third-Party Assessments  
Rationale: Information Asset Protection Controls  
Compliance: Information Asset Protection Controls  
Communication of Findings  
Internal Processes for Incident Response  
Organizational/Third-Party Incident Reports  
Breach Recognition, Notification, Initial Response  
Trust Models for Third-Party Interconnections  
Technical Standards

Connection Agreements  
Information Flow Mapping and Scope  
Data Sensitivity and Classification  
Privacy Requirements  
Security Requirements  
Risks Associated with Third-Parties  
Risk Treatment Identification  
Corrective Action Plans  
Compliance Activities Documentation  
Organizational Breach Notification Rules  
Organizational Information Dissemination  
Policies and Standards  
Risk Assessment Activities  
Chain of Custody  
C)HISSP Course Review